L Number	Hits	Search Text	DB	Time stamp
5	0	("(keyadjdistribut$3adj(centerorunit))").PN	USPAT; US-PGPUB; EPO; DERWENT	2004/07/19 07:04
6	259	(key adj distribut$3 adj (center or unit))	USPAT; US-PGPUB	2004/07/19 07:04
7	38	((key adj distribut$3 adj (center or unit))) and (generat$3 near3 (public adj key$1))	USPAT; US-PGPUB	2004/07/19 07:28
8	4	(((key adj distribut$3 adj (center or unit))) and (generat$3 near3 (public adj key$1))) and (encrypt$1 near3 (session adj key$1))	USPAT; US-PGPUB	2004/07/19 07:29
9	42	((key adj distribut$3 adj (center or unit))) and (distribut$3 near3 (public adj key$1))	USPAT; US-PGPUB	2004/07/19 07:12
10	7	(((key adj distribut$3 adj (center or unit))) and (distribut$3 near3 (public adj key$1))) and (key adj encrypt$3 adj key)	USPAT; US-PGPUB	2004/07/19 07:12
11	69	((key adj distribut$3 adj (center or unit))) and ((generat$3 or distribut$3 or communicat$3) near3 (public adj key$1))	USPAT; US-PGPUB	2004/07/19 07:29
12	4	(((key adj distribut$3 adj (center or unit))) and ((generat$3 or distribut$3 or communicat$3) near3 (public adj key$1))) and (encrypt$1 near3 (session adj key$1) with (public adj key$1))	USPAT; US-PGPUB	2004/07/19 07:38
13	27	(((key adj distribut$3 adj (center or unit))) and ((generat$3 or distribut$3 or communicat$3) near3 (public adj key$1))) and (encrypt$1 near3 key$1 with (public adj key$1))	USPAT; US-PGPUB	2004/07/19 07:38

-	48	("5907618" "5633929" "6058188" "5937066" "5812764" "6449473" "6473508" "5799086" "5841865" "5850451" "5857022" "5872849" "5982898" "6009177" "6389136" "5481613" "5796830" "6052469" "6052466" "6151395" "5815573" "6246771" "6317700" "5708711" "6122742" "6160891" "6202150" "5920630" "6243466" "5633928" "6282295" "6483921" "6260142" "6041123" "6061454" "6061454" "6397329" "6396929" "5557346" "5557765" "5640454" "5956403" "5289542" "6226383" "6226383" "6055636" "5721777" "6742116" "6684331" "6266421").pn.	USPAT; US-PGPUB	2004/07/16 10:03

-	23	(("5907618" "5633929" "6058188" "5937066" "5812764" "6449473" "6473508" "5799086" "5841865" "5850451" "5857022" "5872849" "5982898" "6009177" "6389136" "5481613" "5796830" "6052469" "6052466" "6151395" "5815573" "6246771" "6317700" "5708711" "6122742" "6160891" "6202150" "5920630" "6243466" "5633928" "6282295" "6483921" "6260142" "6041123" "6061454" "6061454" "6397329" "6396929" "5557346" "5557765" "5640454" "5956403" "5289542" "6226383" "6226383" "6055636" "5721777" "6742116" "6684331" "6266421").pn.) and (escrow near1 agent)	USPAT; US-PGPUB	2004/07/15 07:19

-	23	((("5907618" "5633929" "6058188" "5937066" "5812764" "6449473" "6473508" "5799086" "5841865" "5850451" "5857022" "5872849" "5982898" "6009177" "6389136" "5481613" "5796830" "6052469" "6052466" "6151395" "5815573" "6246771" "6317700" "5708711" "6122742" "6160891" "6202150" "5920630" "6243466" "5633928" "6282295" "6483921" "6260142" "6041123" "6061454" "6061454" "6397329" "6396929" "5557346" "5557765" "5640454" "5956403" "5289542" "6226383" "6226383" "6055636" "5721777" "6742116" "6684331" "6266421").pn.) and (escrow near1 agent)) and (public adj key)	USPAT; US-PGPUB	2004/07/15 08:40

-	17	(((("5907618" "5633929" "6058188" "5937066" "5812764" "6449473" "6473508" "5799086" "5841865" "5850451" "5857022" "5872849" "5982898" "6009177" "6389136" "5481613" "5796830" "6052469" "6052466" "6151395" "5815573" "6246771" "6317700" "5708711" "6122742" "6160891" "6202150" "5920630" "6243466" "5633928" "6282295" "6483921" "6260142" "6041123" "6061454" "6061454" "6397329" "6396929" "5557346" "5557765" "5640454" "5956403" "5289542" "6226383" "6226383" "6055636" "5721777" "6742116" "6684331" "6266421").pn.) and (escrow near1 agent)) and (public adj key)) and (common or central)	USPAT; US-PGPUB	2004/07/15 07:24

-	2	(((("5907618" "5633929" "6058188" "5937066" "5812764" "6449473" "6473508" "5799086" "5841865" "5850451" "5857022" "5872849" "5982898" "6009177" "6389136" "5481613" "5796830" "6052469" "6052466" "6151395" "5815573" "6246771" "6317700" "5708711" "6122742" "6160891" "6202150" "5920630" "6243466" "5633928" "6282295" "6483921" "6260142" "6041123" "6061454" "6061454" "6397329" "6396929" "5557346" "5557765" "5640454" "5956403" "5289542" "6226383" "6226383" "6055636" "5721777" "6742116" "6684331" "6266421").pn.) and (escrow near1 agent)) and (public adj key)) and (key near1 updat$3)	USPAT; US-PGPUB	2004/07/15 07:27

-	9	(((("5907618" "5633929" "6058188" "5937066" "5812764" "6449473" "6473508" "5799086" "5841865" "5850451" "5857022" "5872849" "5982898" "6009177" "6389136" "5481613" "5796830" "6052469" "6052466" "6151395" "5815573" "6246771" "6317700" "5708711" "6122742" "6160891" "6202150" "5920630" "6243466" "5633928" "6282295" "6483921" "6260142" "6041123" "6061454" "6061454" "6397329" "6396929" "5557346" "5557765" "5640454" "5956403" "5289542" "6226383" "6226383" "6055636" "5721777" "6742116" "6684331" "6266421").pn.) and (escrow nearl agent)) and (public adj key)) and (interval with (key or index))	USPAT; US-PGPUB	2004/07/15 07:33

-	19	((("5907618" "5633929" "6058188" "5937066" "5812764" "6449473" "6473508" "5799086" "5841865" "5850451" "5857022" "5872849" "5982898" "6009177" "6389136" "5481613" "5796830" "6052469" "6052466" "6151395" "5815573" "6246771" "6317700" "5708711" "6122742" "6160891" "6202150" "5920630" "6243466" "5633928" "6282295" "6483921" "6260142" "6041123" "6061454" "6061454" "6397329" "6396929" "5557346" "5557765" "5640454" "5956403" "5289542" "6226383" "6226383" "6055636" "5721777" "6742116" "6684331" "6266421").pn.) and (escrow near1 agent)) and encrypt$3 same (session near1 key) same (public near1 key)	USPAT; US-PGPUB	2004/07/15 07:55

-	19	((("5907618" "5633929" "6058188" "5937066" "5812764" "6449473" "6473508" "5799086" "5841865" "5850451" "5857022" "5872849" "5982898" "6009177" "6389136" "5481613" "5796830" "6052469" "6052466" "6151395" "5815573" "6246771" "6317700" "5708711" "6122742" "6160891" "6202150" "5920630" "6243466" "5633928" "6282295" "6483921" "6260142" "6041123" "6061454" "6061454" "6397329" "6396929" "5557346" "5557765" "5640454" "5956403" "5289542" "6226383" "6226383" "6055636" "5721777" "6742116" "6684331" "6266421").pn.) and (escrow near1 agent)) and (encrypt$3 same (session near1 key) same (public near1 key))	USPAT; US-PGPUB	2004/07/15 08:23

-	17	((("5907618" "5633929" "6058188" "5937066" "5812764" "6449473" "6473508" "5799086" "5841865" "5850451" "5857022" "5872849" "5982898" "6009177" "6389136" "5481613" "5796830" "6052469" "6052466" "6151395" "5815573" "6246771" "6317700" "5708711" "6122742" "6160891" "6202150" "5920630" "6243466" "5633928" "6282295" "6483921" "6260142" "6041123" "6061454" "6061454" "6397329" "6396929" "5557346" "5557765" "5640454" "5956403" "5289542" "6226383" "6226383" "6055636" "5721777" "6742116" "6684331" "6266421").pn.) and (escrow near1 agent)) and (encrypt$3 with (session near1 key) with (public near1 key))	USPAT; US-PGPUB	2004/07/15 08:39
-	59	380/$.ccls. and (escrow near1 agent)	USPAT; US-PGPUB	2004/07/15 08:41
-	9458	380/$.ccls.	USPAT; US-PGPUB	2004/07/15 08:41
-	35	380/$.ccls. and ((escrow near1 agent) with (public adj key))	USPAT; US-PGPUB	2004/07/15 08:43
-	137	380/$.ccls. and (start$3 near1 key)	USPAT; US-PGPUB	2004/07/15 08:45
-	0	(380/$.ccls. and ((escrow near1 agent) with (public adj key))) and (380/$.ccls. and (start$3 near1 key))	USPAT; US-PGPUB	2004/07/15 08:44
-	388	380/$.ccls. and (interval with key)	USPAT; US-PGPUB	2004/07/15 11:49
-	13	(380/$.ccls. and ((escrow near1 agent) with (public adj key))) and (380/$.ccls. and (interval with key))	USPAT; US-PGPUB	2004/07/15 08:45
-	0	"Diffie-Hellman" and "middle adj attack"	USPAT; US-PGPUB	2004/07/15 11:50

-	0	"Diffie Hellman" and "middle adj attack$1"	USPAT; US-PGPUB	2004/07/15 12:01
-	217	(key adj encrypt$3 adj key) with generat$3	USPAT; US-PGPUB	2004/07/15 14:26
-	16	((key adj encrypt$3 adj key) with generat$3) and (encrypt$3 with index$2 with key$1)	USPAT; US-PGPUB	2004/07/15 13:37
-	0	(key adj encrypt$3 adj key) with (generat$3 or creat$3) with iterative$2	USPAT; US-PGPUB	2004/07/16 07:09
-	23	((key adj encrypt$3 adj key) with generat$3) and (encrypt$3 with (index$2 or label$1 or tag$1) with key$1)	USPAT; US-PGPUB	2004/07/15 14:27
-	58	CATV and (session adj key$1)	USPAT; US-PGPUB	2004/07/15 14:21
-	26	(CATV and (session adj key$1)) and interval	USPAT; US-PGPUB	2004/07/15 14:25
-	20008	713/$.ccls.	USPAT; US-PGPUB	2004/07/15 14:26
-	97	713/$.ccls. and ((key adj encrypt$3 adj key) with generat$3)	USPAT; US-PGPUB	2004/07/15 14:26
-	9	(713/$.ccls. and ((key adj encrypt$3 adj key) with generat$3)) and (encrypt$3 with (index$2 or label$1 or tag$1) with key$1)	USPAT; US-PGPUB	2004/07/15 14:34
-	1	4731840.pn.	USPAT; US-PGPUB	2004/07/15 14:30
-	1	"6691229"	USPAT; US-PGPUB	2004/07/15 14:34
-	0	(key adj encrypt$3 adj key$1) same (generat$3 or creat$3) same iterative$2	USPAT; US-PGPUB	2004/07/16 07:13
-	424	(key adj encrypt$3 adj key$1) same (generat$3 or creat$3)	USPAT; US-PGPUB	2004/07/16 08:55
-	25	((key adj encrypt$3 adj key$1) same (generat$3 or creat$3)) and (key$1 near3 interval$1)	USPAT; US-PGPUB	2004/07/16 08:38
-	0	(key adj encrypt$3 adj key$1) same (generat$3 or creat$3) same iterat$5	USPAT; US-PGPUB	2004/07/16 07:13
-	1	(((key adj encrypt$3 adj key$1) same (generat$3 or creat$3)) and (key$1 near3 interval$1)) and ((start$3 or initial) adj key)	USPAT; US-PGPUB	2004/07/16 08:42
-	1	(((key adj encrypt$3 adj key$1) same (generat$3 or creat$3)) and (video-on-demand or VOD)) and ((start$3 or initial) adj key)	USPAT; US-PGPUB	2004/07/16 08:47
-	7	((key adj encrypt$3 adj key$1) same (generat$3 or creat$3)) and (video-on-demand or VOD)	USPAT; US-PGPUB	2004/07/16 08:46
-	415	(multiple with key$1) same index$2	USPAT; US-PGPUB	2004/07/16 08:47
-	77	((multiple with key$1) same index$2) and encrypt$3	USPAT; US-PGPUB	2004/07/16 08:47
-	3	(((multiple with key$1) same index$2) and encrypt$3) and ((start$3 or initial) adj key)	USPAT; US-PGPUB	2004/07/16 08:54
-	237	middle adj attack$1	USPAT; US-PGPUB	2004/07/16 08:54
-	7	(middle adj attack$1) and (key adj encrypt$3 adj key$1) same (generat$3 or creat$3)	USPAT; US-PGPUB	2004/07/16 08:55
-	1	("6731758").PN.	USPAT; US-PGPUB	2004/07/16 10:49
-	124	((encrypt$3 or cipher$3) adj (label$1 or tag$1 or index$2))	USPAT; US-PGPUB	2004/07/16 13:23
-	20	(((encrypt$3 or cipher$3) adj (label$1 or tag$1 or index$2))) and (key near1 distribut$3)	USPAT; US-PGPUB	2004/07/16 13:15
-	25	((encrypt or cipher) adj (label or tag or index))	USPAT; US-PGPUB	2004/07/16 13:47
-	0	("WO57595").PN.	USPAT; US-PGPUB; EPO; DERWENT	2004/07/16 14:31

-	1	("0057595").PN.	USPAT; US-PGPUB; EPO; DERWENT	2004/07/16 14:32
-	2	("200057595").PN.	USPAT; US-PGPUB; EPO; DERWENT	2004/07/19 07:03

Scientific & Technical Information Center
STIC
USPTO

STIC EIC 2100 127359
Search Request Form

Today's Date: 7/15/04
09/757742

What date would you like to use to limit the search?
Priority Date: Jan 9, 2001 Other:

Name Minh D. Nguyen
AU 2137 Examiner # 79995
Room # PK2 4R20 Phone
Serial # 09/757742

Format for Search Results (Circle One):
PAPER DISK EMAIL

Where have you searched so far?
USP DWPI EPO JPO ACM IBM TDB
IEEE INSPEC SPI Other

Is this a "Fast & Focused" Search Request? (Circle One) YES NO
A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC2100 and on the EIC2100 NPL Web Page at http://ptoweb/patents/stic/stic-tc2100.htm.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

* 3rd party distribution center to distribute public keys

* key encryption key iteratively generating not (distributing, transporting or storing) in interval (time).

* encrypt indexes or labels or tags that are tied with key.

*

STIC Searcher Geoffrey St Leger Phone 308-7800
Date picked up 7/15/4 Date Completed 7/16/4

sira
Search and Information Resources Administration

```
File 348:EUROPEAN PATENTS 1978-2004/Jul W01
         (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040708,UT=20040701
         (c) 2004 WIPO/Univentio

Set     Items   Description
S1       2040   (COMMON OR SHARED)(2W)KEY? ?
S2     207232   INDEX OR INDEXES OR INDICES OR SCHEDULE? ? OR TIME()TABLE?
             ?
S3      30766   KEY? ?(5N)(ESTABLISH? OR GENERAT? OR CREAT???? OR FASHION?
             OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR PRODUC?-
             ???? OR DEVELOP? OR BUILT OR BUILD?)
S4      12611   KEY? ?(5N)(COMPUTE OR COMPUTES OR COMPUTED OR COMPUTING OR
             DETERMIN? OR DISCERN? OR DERIV??? OR DERIVATION OR CALCULA?)
S5      37950   CRYPTO? OR CRYPTANALY? OR CIPHER? OR CYPHER? OR ENCRYPT? OR
              ENCIPHER? OR DECRYPT? OR DECIPHER? OR UNENCRYPT?
S6     842257   TIMES OR INTERVAL? ? OR PERIOD?
S7         27   S1(50N)S2(50N)S3:S4(50N)S5(50N)S6
S8       6538   PUBLIC()KEY? ?
S9         68   S1(50N)S3:S4(50N)S6(50N)S8
S10        63   S9 NOT S7
S11        27   S10 AND AC=US/PR
S12        27   S11 AND AY=(1970:2001)/PR
S13        45   S10 AND PY=1970:2001
```

7/5,K/19 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00802583 **Image available**
METHOD AND APPARATUS FOR RE-SYNCHRONIZATION OF A STREAM CIPHER DURING HANDOFF
PROCEDE ET APPAREIL PERMETTANT DE RESYNCHRONISER UN ALGORITHME DE CHIFFREMENT EN CONTINU PENDANT UN TRANSFERT
Patent Applicant/Assignee:
QUALCOMM INCORPORATED, 5775 Morehouse Drive, San Diego, CA 92121-1714, US , US (Residence), US (Nationality)
Inventor(s):
ROSE Gregory D, 6 Kingston Avenue, Mortlake, NSW 2137, AU,
Legal Representative:
WADSWORTH Philip R (et al) (agent), Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200135681 A2-A3 20010517 (WO 0135681)
Application: WO 2000US31198 20001113 (PCT/WO US0031198)
Priority Application: US 99438341 19991111
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-009/12
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 4623

English Abstract
The present invention is directed to a method and apparatus for securely re-synchronizing a stream cipher while a mobile station is travelling from the range of a fist base station to a second base station. In one aspect of the invention, a secret key and a unique non-secret key are used to reinitialize the stream cipher used by the mobile station. (The unique non-secret key can also be referred to as quasi-secret key). A quasi-secret key is transmitted from a fist base station to a second base station, and the second base station uses the quasi-secret key to initialize a stream cypher generator. Hence, both the mobile station and the second base station will start generating the stream cipher from the same initial state. In another aspect of the invention, a secret key and a quasi-secret key are used to create a new key. During a soft handoff process, a quasi-secret key is transmitted from a fist base station to a second base station. The second base station uses the quasi-secret key and a secret key to generate a new key. The mobile station and the second base station use the new key to generate a new stream cipher for encrypting the data streamflowing between the mobile station and the second base station.

French Abstract
L'invention concerne un procede et un appareil permettant de resynchroniser un chiffrement en continu pendant un transfert en douceur. Les informations de chiffrement quasi-secretes transmises sont utilisees avec une cle secrete, afin de reinitialiser un generateur de chiffrement en continu situe dans une station de base et un generateur de chiffrement en continu situe dans une station mobile. Du fait que les informations de chiffrement quasi-secretes sont determinees uniquement en fonction de chaque station de base du systeme telephonique sans fil, il est egalement possible d'utiliser une information de chiffrement de station de base quasi-secrete et une cle de cryptage partagee pour creer une nouvelle

cle. En consequence, lorsque la station mobile se deplace d'une station de base vers une autre station de base, une nouvelle cle unique est generee pour chaque station de base.

Legal Status (Type, Date, Text)

Publication	20010517	A2 Without international search report and to be republished upon receipt of that report.
Examination	20010927	Request for preliminary examination prior to end of 19th month from priority date
Search Rpt	20011122	Late publication of international search report
Republication	20011122	A3 With international search report.

Fulltext Availability:
Detailed Description

Detailed Description

... transmission end 5 combined with a subtraction operation on the receiving end 6.

For the **encryption** and **decryption** process of FIG. I to work, there must
be synchronization between the transmission end 5 and the receiving end 6.
Each bit of the **encrypted** data stream must be XORed with the correct, corresponding bit of the stream **cipher** . Otherwise, the output will not correspond to the original data.

In some circumstances, restarting or regenerating the stream **cipher** at the receiving end 6 requires an avoidable use of system resources. One method of generating stream **ciphers** efficiently is disclosed in U.S. Patent Application
No. 08/934,582, filed September 22, 1997, entitled "METHOD AND APPARATUS FOR GENERATING **ENCRYPT1ON** STREAM **CIPHERS** ,"
assigned to the assignee of the present invention, and incorporated by reference herein.

In one embodiment of the invention, a stream **cipher** can be generated with a linear feedback shift register. A linear feedback shift register holds...

...current state that consists of k elements from some finite field. If the starting states (**derived** directly from the **shared** secret **key**) are known and the number of **times** by which the linear feedback shift registers have been cycled is also known, then the registers can be updated to the state to which the **encrypted** data stream currently corresponds.

When a register is cycled, a new element of the register...

...k is a constant indicating the order of the recurrence relation, and n is an **index** in time. The state variables S and coefficients Ci are elements of the underlying finite...

7/9/21 **(Item 9 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT

00744205 **Image available**
METHOD AND APPARATUS FOR ENCRYPTING AND DECRYPTING DATA
PROCEDE ET APPAREIL DE CHIFFRAGE ET DE DECHIFFRAGE DES DONNEES
Patent Applicant/Assignee:
KENT RIDGE DIGITAL LABS, 21 Heng Mui Keng Terrace, Singapore 119613, SG, SG (Residence), SG (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
BAO Feng, 37 West Coast Park, #04-06, Parkview Condo, Singapore 127653, SG, SG (Residence), CN (Nationality), (Designated only for: US)
DENG Huijie Robert, 2 Namly Rise, Singapore 267110, SG, SG (Residence), SG (Nationality), (Designated only for: US)
Legal Representative:
HELEN YEO & PARTNERS, 80 Raffles Place, #33-00 UOB Plaza 1, Singapore 048624, SG
Patent and Priority Information (Country, Number, Date):
Patent: WO 200057595 A1 20000928 (WO 0057595)
Application: WO 99SG20 19990322 (PCT/WO SG9900020)
Designated States: JP SG US
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: H04L-009/00
Publication Language: English
Filing Language: English
Fulltext Word Count: 5303

English Abstract
A method and apparatus for encrypting and decrypting data is disclosed which employs two or more cryptographic algorithms to achieve high throughput without compromizing security. The invention is especially useful for software implementation to protect large amounts of multimedia data over high-speed communication channels.

French Abstract
L'invention concerne un procede et un appareil de chiffrage et de dechiffrage de donnees. Ce procede utilise au moins deux algorithmes cryptographiques pour obtenir un rendement eleve sans nuire a la securite. L'invention est particulierement utile pour la realisation logicielle en vue de proteger de grandes quantites de donnees multimedia passant par des canaux de communication haute vitesse.

Legal Status (Type, Date, Text)
Publication 20000928 A1 With international search report.
Publication 20000928 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20001123 Request for preliminary examination prior to end of 19th month from priority date

Detailed Description
METHOD AND APPARATUS FOR
ENCRYPTING AND DECRYPTING DATA
FIELD OF THE INVENTION
The present invention relates to cryptography and in particular to a method and apparatus for encrypting and decrypting digital data for the purpose of protecting or securing its contents.

BACKGROUND OF THE INVENTION
There exists a need to transfer data confidentially over an open channel or to store such data securely in an unsecure location. Whilst such transfer or storage may be achieved by physical means, it is more effective and/or flexible to use cryptographic means.

In the prior art, to send private communications between two parties, the parties need to share a cryptographic key and use a symmetric-key cipher

to encrypt and decrypt data. Various ciphers including block ciphers and stream ciphers have been proposed in the past. A stream cipher handles messages of arbitrary size by ciphering individual elements, such as bits or bytes of data. This avoids the need to accumulate data into a block before ciphering as is necessary in a block cipher. A conventional block cipher requires an accumulation of a certain amount of data or multiple data elements for ciphering to complete. Examples of block ciphers include DES (see ANSI X3.92, "American National Standard for Data Encryption Algorithm (DEA)," American National Standards Institute, 1981), IDEA, (see X. Lai, J. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis," Advances in Cryptology - EUROCRYPT'91 Proceedings, Springer-Veriag, 1991, pp. 17-38), SAFER (see J. Massey. SAFER K-64: One year later. In B. Preneel, editor, Fast Software Encryption - Proceedings of Second International Workshop, LNCS 1008, pages 212-241, Springer Verlag, 1995), and RC5 (see R. Rivest, "The RC5 encryption algorithm," Dr. Dobb's Journal, Vol. 20, No. 1 , January 1995, pp. 146 -148). A typical data encryption speed for these ciphers is several million bits per second (Mb/s) on a Pentium 266 MHz processor.

Due to the pervasiveness of high-speed networking and multimedia communications, the demand for high-speed ciphers is ever increasing. For example, data rates over Asynchronous Data Transfer networks range from several tens of Mb/s to 1 Gb/s. Software implementations of existing block ciphers cannot reach these kinds of data rates.

In general, stream ciphers are much faster than block ciphers. However, stream ciphers are usually not sufficiently analyzed and are perceived to be weaker in security than block ciphers. Many stream ciphers that we believed to be very secure were subsequently broken. The design of secure and efficient high-speed ciphers remains a highly challenging problem.

Many powerful cryptanalytical methods have been developed during the past decade or so. It may be observed that the success of many of these methods in attacking a cipher depends on the availability of a large quantity of ciphertexts/plaintenxts under a particular encryption key. Normally, the likelihood of successfully attacking a cipher, i.e., discovering the key, diminishes as the amount of available ciphertexts/plaintexts decreases. The present invention, is motivated by the above observation, and provides an improved method and apparatus for data encryption and decryption.

SUMMARY OF THE INVENTION

The method of the present invention may employ a combination of at least two cryptographic algorithms to achieve relatively high throughput without compromizing security. A first algorithm may be a cryptographic pseudo random sequence (or number) generator with strong security, and a second algorithm may be a cipher capable of high-speed operation, but may be weak in security when used alone. The first algorithm may be used to systematically and periodically generate "segment keys" and the second algorithm may be used to encrypt a data segment or plaintext segment using a segment key. Each data segment may be encrypted using a different segment key. By limiting the sizes of the data segments, an attacker may not have sufficient plaintexts or ciphertexts under a given segment key to carry out meaningful cryptanalysis against the second algorithm. In doing so, the present invention may achieve high throughput in data encryption and decryption without compromizing overall security of the system.

According to one aspect of the present invention there is provided a method of encrypting data suitable for sending to a decrypting party, said method including the steps of.
(a) dividing said data into data segments;
(b) accepting at least a cryptographic key k shared with the decrypting

party;
(c) for the Ah data segment (i = 11 21 ...) to be encrypted, generating the Ah segment key si using a first function with said cryptographic key k and some accessory data strings as inputs;
(d) encrypting the Ah data segment using a second function with si as the encryption key to form the Ah ciphertext segment; and
(e) outputting the Ah ciphertext segment, and at least a part of said accessory data strings for sending data to the decrypting party, and if more data segments are to be encrypted, repeating steps (c), (d) and (e).

The accessory data strings may include a single string vi derived from the previous value vi-1 in a predetermined fashion. The string vi may be derived according to the relation yj = F(vi-1), i = 1 1 21 ... , wherein F(maps vi-1 to yj and vo is an initialization value made known to the decrypting party.

According to a further aspect of the present invention there is provided a method of decrypting data encrypted by an encrypting party, said method including the steps of.
(a) accepting at least a cryptographic key k being shared with the encrypting party;
(b) for the Ah ciphertext segment (i = 1, 2, ...,) to be decrypted, generating the Ah segment key si using a first function with said Cryptographi c key k and some accessory data strings as inputs;
(c) decrypting the hh ciphertext segment using a second function with si as the decryption key;
(d) outputting the decrypted Ah ciphertext segment, and if more ciphertext segments are to be decrypted, repeating steps (b), (c) and (d).

According to a still further aspect of the present invention there is provided apparatus for encrypting data suitable for sending to a decrypting party, said apparatus including.

(a) means for dividing said data into data segments;
(b) means for accepting at least a cryptographic key k shared with the decrypting party;
(c) means for generating for the Ah data segment (i = 11 21 ...) to be encrypted, the Ah segment key si using a first function with said cryptographic key k and some accessory data strings as inputs;
(d) means for encrypting the Ah data segment using a second function with si as the encryption key to form the hh ciphertext segment; and
(e) means for outputting the Ah ciphertext segment, and at least a part of said accessory data strings for sending data to the decrypting party.

According to a still further aspect of the present invention there is provided apparatus for decrypting data encrypted by an encrypting party, said apparatus.

including.

(a) means for accepting at least a cryptographic key k being shared with the encrypting party;
(b) means for generating as inputs for the Ah ciphertext segment (i = 1 1 2, ...,) to be decrypted, the Ah segment key si using a first function with said cryptographic key k and some accessory data strings;
(c) means for decrypting the Ah ciphertext segment using a second function with si as the decryption key; and
(d) means for outputting the decrypted hh ciphertext segment.

```
File   8:Ei Compendex(R) 1970-2004/Jul W1
         (c) 2004 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2004/May
         (c) 2004 ProQuest Info&Learning
File  65:Inside Conferences 1993-2004/Jul W2
         (c) 2004 BLDSC all rts. reserv.
File   2:INSPEC 1969-2004/Jul W1
         (c) 2004 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2004/Jun W4
         (c)2004 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2004/Jul W3
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2004/Jul W1
         (c) 2004 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2004/Jul W2
         (c) 2004 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Jun
         (c) 2004 The HW Wilson Co.
File 266:FEDRIP 2004/May
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  95:TEME-Technology & Management 1989-2004/Jun W1
         (c) 2004 FIZ TECHNIK
File 104:AeroBase 1999-2004/Jun
         (c) 2004 Contains copyrighted material
File  62:SPIN(R) 1975-2004/May W3
         (c) 2004 American Institute of Physics
File 239:Mathsci 1940-2004/Sep
         (c) 2004 American Mathematical Society

Set      Items   Description
S1        1345   (COMMON OR SHARED)(2W)KEY? ?
S2     1370908   INDEX OR INDEXES OR INDICES OR SCHEDULE? ? OR TIME()TABLE?
             ? OR TIMETABLE
S3       75768   KEY? ?(5N)(ESTABLISH? OR GENERAT? OR CREAT???? OR FASHION?
             OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR PRODUC?-
             ???? OR DEVELOP? OR BUILT OR BUILD?)
S4       24347   KEY? ?(5N)(COMPUTE OR COMPUTES OR COMPUTED OR COMPUTING OR
             DETERMIN? OR DISCERN? OR DERIV? OR CALCULA?)
S5      160201   CRYPTO? OR CRYPTANALY? OR CIPHER? OR CYPHER? OR ENCRYPT? OR
               ENCIPHER? OR DECRYPT? OR DECIPHER? OR UNENCRYPT?
S6     4093743   TIMES OR INTERVAL? ? OR PERIOD?
S7           0   S1 AND S2 AND S3:S4 AND S5 AND S6
S8          26   S1 AND S3:S4 AND S6
S9          14   RD (unique items)
S10          6   S9 NOT PY=2002:2004
S11          0   S1 AND S2 AND S5 AND S6
S12          9   S2 AND S3:S4 AND S5 AND S6
S13          9   RD (unique items)
```

13/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

06763705 E.I. No: EIP04128069147
Title: A New Steganographic Method for Palette-Based Images
Author: Fridrich, Jiri
Corporate Source: Center for Intelligent Systems SUNY Binghamton, Binghamton, NY, United States
Conference Title: Final Program and Proceedings: IS and T's 52nd Annual Conference
Conference Location: Savannah, GA, United States Conference Date: 19990425-19990428
E.I. Conference No.: 62399
Source: Society for Imaging Science and Technology: Image Processing, Image Quality, Image Capture, Systems Conference 1999.
Publication Year: 1999
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 0403W4
Abstract: In this paper, we present a new steganographic technique for embedding messages in palette-based images, such as GIF files. The new technique embeds one message bit into one pixel (its pointer to the palette). The pixels for message embedding are chosen randomly using a pseudo-random number **generator** seeded with a secret **key** . For each pixel at which one message bit is to be embedded, the palette is searched for closest colors. The closest color with the same parity as the message bit is then used instead of the original color. This has the advantage that both the overall change due to message embedding and the maximal change in colors of pixels is smaller than in methods that perturb the least significant bit of **indices** to a luminance-sorted palette, such as EZ Stego.**1 Indeed, numerical experiments indicate that the new technique introduces approximately four **times** less distortion to the carrier image than EZ Stego. The maximal color change is 4-5 **times** smaller for the new technique than that of EZ Stego. A technique that introduces less distortion to the carrier image will generally cause changes that are more difficult to detect, and will therefore provide more security. 6 Refs.
Descriptors: Image quality; Security of data; Quantum **cryptography** ; Imaging systems; Cosine transforms; Fourier transforms
Identifiers: Steganographic methods; Digital images
Classification Codes:
723.2 (Data Processing); 921.3 (Mathematical Transformations)
741 (Light, Optics & Optical Devices); 723 (Computer Software, Data Handling & Applications); 921 (Applied Mathematics)
74 (LIGHT & OPTICAL TECHNOLOGY); 72 (COMPUTERS & DATA PROCESSING); 92 (ENGINEERING MATHEMATICS)

13/5/2 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

1040427 ORDER NO: AAD89-02312
ABSTRACT TIMING VERIFICATION FOR SYNCHRONOUS DIGITAL SYSTEMS
Author: WALLACE, DAVID EDWARD
Degree: PH.D.
Year: 1988
Corporate Source/Institution: UNIVERSITY OF CALIFORNIA, BERKELEY (0028)
CHAIRMAN: CARLO H. SEQUIN
Source: VOLUME 49/11-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 4909. 251 PAGES
Descriptors: COMPUTER SCIENCE; ENGINEERING, ELECTRONICS AND ELECTRICAL
Descriptor Codes: 0984; 0544

ATV, the Abstract Timing Verifier, is a program to perform static timing analysis of dependency graphs derived from logic designs, analyzing worst-case paths. Unlike other timing verifiers, ATV uses an abstract representation of time and delays that enables a user to choose the

representation of time and delays used in the analysis. Such representations include single numbers, ranges (min-max), and statistical descriptions (mean and standard deviation), or asymmetric rise/fall versions of all of these. The sophisticated user may develop new models and plug them in to the program.

ATV uses a new algorithm to analyze critical paths that extend through transparent latches and stretch over multiple machine cycles. By placing events in different reference frames that are rigidly translated relative to one another, the program can be used either to check a design for timing errors when the clock **schedule** is fixed and known, or to derive spacing constraints between clock edges when only the relative ordering of the clock edges is known.

By defining coercions between delay formats, the same raw data can be analyzed using several different timing models to determine the sensitivity of reported results to the assumptions made by the different models. In one analysis of a chip implementing the Data **Encryption** Standard, six different timing models reported as many as 14 and as few as 4 critical paths **generating** the same **key** event. In general, asymmetric rise/fall models generated more critical paths because of interactions between reconvergent paths of opposite polarity. As expected, min-max models tended to be the most conservative in estimating required cycle **times** , single-number models using nominal values were the most optimistic, and probabilistic models were in between.

ATV is designed to operate on generic dependency information that could be available early in the design cycle, providing early feedback about the timing implications of microarchitectural decisions. The framework it provides allows new timing models to be developed and compared with existing models on an equal basis. The development of the abstract timing model has led to new understandings of the similarities and differences between the many different timing models in use today.

13/5/4 (Item 1 from file: 239)

DIALOG(R)File 239:Mathsci

03222340 MR 2001m#94049

Cryptography **in quadratic function fields.**

Scheidler, R. (Department of Mathematics, University of Delaware, Newark, Delaware, 19716)
Corporate Source Codes: 1-DE

Des. Codes Cryptogr.
Designs, Codes and Cryptography. An International Journal, 2001, 22, no. 3, 239--264. ISSN: 0925-1022 CODEN: DCCREC
Language: English Summary Language: English
Document Type: Journal
Journal Announcement: 200109
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: LONG (143 lines)

In this paper the author presents key exchange protocols, public-key **cryptosystems** , and signature schemes in quadratic function fields of odd characteristic. The **cryptographic** protocols differ depending upon whether the quadratic function field is real or imaginary, where we recall that a quadratic function field K is defined as $K=k(t,y)$ where t is transcendental over k and $y\sp {2}=D$ with $D=D(t)$ a (squarefree) polynomial in t having coefficients in k. K is real provided $\deg(D)=2g+2$ is even (g the genus of the elliptic or hyperelliptic curve C used to define K) and the leading coefficient of D is a square in k, and is imaginary otherwise (the case where K is imaginary with $\deg(D)$ even and the leading coefficient nonsquare is real quadratic over a quadratic extension of k, so when K is imaginary we may take $\deg(D)$ to be odd, specifically having degree $2g+1$). The security of the protocols relies on analogous versions of the well-known discrete logarithm problem for finite fields.

Before discussing either case, some definitions are in order. Let $k[t]$ denote the ring of polynomials in t over k with $\scr{O}$ representing the integral closure of $k[t]$ in K. $\scr O$ is a $k[t]$-module of rank 2 with basis $\{1,\sqrt{D}\}$. An integral ideal $\scr{A} \subset

\scr{O}$ is an ideal with the property that for any α, $\beta \in \scr{A}$ and $\theta \in \scr{O}$, $\alpha + \beta \in \scr{A}$ and $\theta\alpha \in \scr{A}$. A fractional ideal $\scr{A}$ is a subset of K such that $d\scr{A}$ is an integral ideal for some nonzero $d \in k[t]$. If the $\scr{O}$-rank of $\scr{A}$ is 1, that is there exists $\alpha \in K$ with $\scr{A}=\{\theta\alpha\colon\ \theta\in\scr{O}\}$, then $\scr{A}$ is a principal ideal with generator α, and we write $\scr{A}=(\alpha)$. Throughout the paper, all ideals are assumed to be nonzero, so that every integral ideal $\scr{A}$ is a $k[t]$-module of rank 2 with $k[t]$-basis $\{SQ,SP+S\sqrt{D}\}$ where $S,Q,P \in k[t]$ with $SQ \neq 0$ and Q dividing $D-P\sp {2}$. (There is a misprint in the paper, namely on page 241, where it is said that Q divides $D\sp {2}-P$; this misprint is not repeated, and the correct difference, namely $D-P\sp {2}$, is used throughout.) Writing $\scr{A}=(SQ,SP)$, we may assume that S and Q are monic with $\deg(P)<\deg(Q)$, so that S, Q, and P are unique. If $\scr{A}$ is primitive, that is $S=1$, with Q monic and $\deg(P)<\deg(Q)$, then (Q,P) is the standard representation of $\scr{A}$, and $\scr{A}$ is said to be in standard form. A primitive ideal $\scr{A}$ is reduced if $\deg(Q) \leq g$. Due to its suitably small representation (in terms of g), the notion of a reduced ideal is central to efficient computation in K, as the author's algorithms demonstrate.

In the imaginary case, the author's **cryptographic** schemes are based on arithmetic in the ideal class group $\scr{C}$ of K, where by the ideal class group we mean the factor group $\scr{I}/\scr{P}$, $\scr{I}$ denoting the infinite abelian group, under multiplication of ideals (the product of $\scr{A},\scr{B} \in \scr{I}$, denoted $\scr{AB}$, consists of all finite sums of products of the form $\alpha\beta$ for $\alpha \in \scr{A}$ and $\beta \in \scr{B}$), of nonzero fractional ideals of K, and $\scr{P}$ the subgroup of nonzero fractional principal ideals of K. The **index** of $\scr{C}$, the ideal class number of K, is finite and denoted by $h\sp {\prime}$. Two fractional ideals $\scr{A}$ and $\scr{B}$ are equivalent if there exists $\theta \in K\sp {\ast}$ with $\scr{A}=(\theta)\scr{B}$, that is $\scr{A}$ and $\scr{B}$ lie in the same coset of $\scr{C}$. Denote this relationship by $\scr{A} \sim \scr{B}$. Every equivalence class of ideals contains at least one and at most finitely many reduced ideals. If K is imaginary, then each class has a unique reduced representative, and this fact can be used to build the algorithms underlying the **cryptographic** schemes. Specifically, letting each class be represented by its reduced representative, one can compute the reduced representative of the product ideal efficiently, even if the product of the reduced ideals is not itself reduced (as it generally will not be). The discrete logarithm problem for the imaginary case, then, is the problem as expressed in $\scr{C}$, namely given reduced ideals $\scr{F}\sb {1}$, $\scr{F}\sb {2}$ with $\scr{F}\sb {1} \sim \scr{F}\sb {2}\sp {x}$ for some integer x, find x mod $h\sp {\prime}$.

The author gives an efficient algorithm to compute a standard representation of a product ideal, where the component ideals are reduced and in standard form; given the product ideal, she also shows how to efficiently determine the reduced representative of the product ideal's class. In particular, the algorithms she provides allow one to calculate the product ideal in $O(g\sp {2})$ field operations (this algorithm can also be applied to the real case); an ideal composition algorithm which outputs the reduced ideal equivalent to the product ideal in standard form, also in $O(g\sp {2})$ field operations; and an exponentiation algorithm based on the square-and-multiply technique, which calculates $\scr{A}\sp {n}$ in $O(\max\{1,g\sp {2}\log n\})$ field operations. These algorithms are then used to **construct** a **key** exchange scheme of Diffie-Hellman type as well as **encryption** and signature schemes of ElGamal type. For the signature scheme, the author demonstrates the necessity of using a collision-free hash function in order to prevent an attack in which the **cryptanalyst** forges the signer's signature by selecting a random positive integer s and using said integer to generate a reduced ideal $(Q\sb {r},P\sb {r})$ equivalent to a valid signature $(Q\sb {r},P\sb {r},s)$. Specifically, by using a hash, the signer must generate a reduced ideal $(Q\sb {r},P\sb {r})$ before computing s, and not vice versa.

The approach for the imaginary case does not carry over to the case of a real quadratic function field, as each ideal class has many reduced representatives. By restricting one's attention to the finite set $\scr{R}

\subset \scr{P}$ of reduced principal ideals, however, one can still construct efficient **cryptographic** schemes. Specifically, one defines the distance of a reduced principal ideal $\scr{A}$ to be the degree of a generator of minimal nonnegative degree. This quantity is denoted by $\delta (\scr{A})$. Further, for nonnegative integer n we say the reduced principal ideal $\scr{A}$ is below n if $n-\delta (\scr{A}) \geq 0$ and minimal. The discrete logarithm problem for this case is as follows: Given reduced principal ideals $\scr{F}\sb {1}$ and $\scr{F}\sb {2}$ so that $\scr{F}\sb {1}$ is the reduced principal ideal below $x\scr{F}\sb {2}$, find x mod R where R is the maximal distance, or regulator, of K. The author shows this problem to be polynomially equivalent to the problem of finding the distance of a reduced principal ideal. As with the imaginary case, she presents efficient algorithms for computing the standard representation of a product ideal as well as determining a reduced representative of its class, with running **times** comparable to those for the imaginary case. Additionally, she shows how to find the reduced principal ideal below n for any nonnegative integer n. The exponentiation algorithm for the real case, based upon algorithms that find reduced ideals and compose two ideals according to the manner described above, is used in the **construction** of **key** exchange and **encryption** protocols, while the exponentiation and ``below'' algorithms are used to form an efficient signature scheme. As with the imaginary case, the key exchange protocol is of Diffie-Hellman type while the public-key **cryptosystem** and signature scheme are each of ElGamal type.

The author concludes with a discussion of the security of the **cryptographic** protocols for both cases. So long as the class group (imaginary case) or the set of reduced principal ideals (real case) is sufficiently large, namely on the order of $q\sp {g}$ for odd prime power q and genus g, the underlying discrete logarithm problems for said protocols can only be solved in exponential time, provided the genus is not too large. This contrasts nicely with the corresponding problem in number fields, where a subexponential algorithm for solving the discrete logarithm problem is available (assuming the extended Riemann hypothesis holds).

Reviewer: Mills, Donald D. (1-WEPT)
Review Type: Signed review
Descriptors: *94A60 -Information and communication, circuits-Communication, information- **Cryptography** (See also 11T71, 14G50, 68P25) ; 11T71 -Number theory-Finite fields and commutative rings (number-theoretic aspects)-Algebraic coding theory; **cryptography** ; 13C20 -Commutative rings and algebras-Theory of modules and ideals-Class groups (See also 11R29

13/5/5 (Item 2 from file: 239)
DIALOG(R)File 239:Mathsci

03195264 MR 2001j#11122
Number theory for computing.
Yan, Song Y. (Department of Computer Science, University of Aston, Birmingham, B4 7ET, England)
Dubner, Harvey
Granlund, Torbjorn
Corporate Source Codes: 4-ASTN-C
Publ: Springer-Verlag, Berlin,
J. Integer Seq.
Journal of Integer Sequences, 2000, 3, no. 2, xviii+381 pp. ISBN: 3-540-65472-0 ISSN: 1530-7638
Price: $46.00.
Language: English Summary Language: English
Document Type: Book
Journal Announcement: 200105
Subfile: MR (Mathematical Reviews) AMS; MR (Mathematical Reviews) AMS
Abstract Length: LONG (59 lines)
When I first saw Yan's new book, I was hopeful that this text might serve as a nice alternative for teaching undergraduate number theory and **cryptography** , a course I have taught several **times** . In the preface, he says that the text is self-contained, and requires no previous background beyond high-school mathematics.

This text is divided into three parts of about 120--130 pages each: Elementary number theory, Algorithmic number theory, and Applied number theory.

Part 1, an overview of elementary number theory, has sections on divisibility (including Euclid's algorithm), Diophantine equations, arithmetic functions, the distribution of primes, congruences (Jacobi symbols, the Chinese remainder theorem), and elliptic curves.

Part 2, on computational and algorithmic number theory, begins with an introduction to computability theory and computational complexity, followed by sections on primality testing, factorization, and discrete logarithms. Next is a section on number-theoretic algorithms for the quantum computer, which I found to be a pleasant surprise. I don't recall seeing any other texts on algorithmic number theory that included this material. Part 2 finishes with sections on algorithms for computing $\pi(x)$, for finding amicable pairs, for verifying Goldbach's conjecture, and for finding odd perfect numbers.

Part 3, on applications of number theory, focuses on two application areas: computer system design (computer arithmetic, hash functions, error detection and correction, and random number **generation**), and **cryptography** (DES, public- **key** **cryptosystems** , digital signatures, and short sections on steganography and quantum **cryptography**).

The book opens with 6 pages of definitions and notation used throughout the text. There is an **index** and a rather thorough, 11-page bibliography.

One very attractive feature is the wealth of historical and biographical information. I did not actually calculate this, but nearly every other page contains a short biography and picture of a famous historical or current personality in the footnotes. For example, on pages 8 and 9 are short biographies of Vinogradov, Chen, and Ramanujan, together with pictures.

I quickly discovered that this text was not appropriate for undergraduates (or, at least not most of the ones I teach). Although there are a few exercises, there are not many; certainly not enough for an undergraduate course. Also, most of the proofs of the theorems used are missing, although plenty of references are included if you want to find the proofs, and finally, the material is too dense for undergraduates.

However, it seems to me this book would be ideal for a graduate student in algorithmic number theory: it provides a nice resource and overview of the field, and the means to find out more. I certainly would have appreciated this text when I was a graduate student, and it is a worthy addition to your library.

Overall, I recommend this book, but I have one minor complaint. Song Yan defines algorithmic number theory and computational number theory to be the same thing (p. 139). In my opinion, which I believe is shared by others, algorithmic number theory is about studying algorithms, whereas computational number theory is about solving problems in number theory using the computer. One is a part of computer science, the other a part of mathematics. I admit, however, that the line between them is thin in some places and blurry in others.

Reviewer: Sorenson, Jonathan P. Wagstaff, Samuel S., Jr. (1-BUTL-CS)

Review Type: Signed review

Descriptors: *11Yxx -Number theory-Computational number theory(See also 11-04); * 11Y11 -Number theory-Computational number theory(See also 11-04)-Primality ; 68P25 -Computer science (For papers involving machine computations and programs in a specific mathematical area, see Section --04 in that area)-Theory of data-Data **encryption** (See also 94A60, 81P68); 68Q05 -Computer science (For papers involving machine computations and programs in a specific mathematical area, see Section --04 in that area)-Theory of computing-Models of computation (Turing machines, etc.) (See also 03D10, 81P68); 68W40 -Computer science (For papers involving machine computations and programs in a specific mathematical area, see Section --04 in that area)-Algorithms (For numerical algorithms, see 65-XX; for combinatorics and graph theory, see 68Rxx)-Analysis of algorithms (See also 68Q25); 94A60 -Information and communication, circuits-Communication, information- **Cryptography** (See also 11T71, 14G50, 68P25); 11A51 -Number theory-Elementary number theory (For analogues in number fields, see 11R04) -Factorization; primality; 11Y55 -Number theory-Computational number theory(See also 11-04)-Calculation of integer sequences

13/5/7 **(Item 4 from file: 239)**
DIALOG(R)File 239:Mathsci

02447216 MR 94f#94007
The stability theory of stream ciphers .
Ding, C.
Xiao, G.
Shan, W.
(Ding, Cun Sheng; Xiao, Guo Zhen)
Publ: Springer-Verlag, Berlin,
1991, x+187 pp. ISBN: 3-540-54973-0
Series: Lecture Notes in Computer Science, 561.
Price: $31.00.
Language: English
Document Type: Book
Journal Announcement: 9314
561
Lecture Notes in Computer Science,
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: LONG (76 lines)
From the introduction: ``This research report is devoted to a new branch of stream **ciphers** : the stability theory of stream **ciphers** . It is mainly based on our research results, which have been obtained since 1987, mainly by Ding. In order to be self-contained, the monograph also presents some known facts which will be useful in our analyses.

``Chapter 2 gives an introduction to stream **ciphers** . Chapter 3 first introduces the two kinds of Walsh transforms and their properties. Then it discusses the best affine approximation of Boolean functions, which will be used as a basic tool for dealing with some problems of some of the following chapters. Finally, it presents the BAA attacks on two classes of stream **ciphers** .

``Chapter 4 mainly introduces several measure **indexes** on the security of stream **ciphers** . Based on the results of Chapter 3, Section 4.1 discusses whether correlation-immune functions are good filtering or combining functions for stream **ciphers** . Section 4.2 first shows some **cryptographic** merits and demerits of bent functions for some binary additive stream **ciphers** , then presents an autocorrelation characterization of bent functions. Section 4.3 introduces new measure **indexes** on the stability of linear complexity of sequences, i.e., weight complexity or sphere surface complexity and sphere complexity, and also presents basic properties of the two measure **indexes** . Section 4.4 analyzes the security of several kinds of **key** -stream **generators** from the viewpoint of the best affine approximation attacks. Section 4.5 provides some results on the stability of elementary symmetric functions, since they are basic components of the GF(2)-interpretation of integer addition, which have been concluded to be useful in both public-key **cryptosystems** and stream **ciphers** .

``Chapter 5 aims at investigating the stability of linear complexity of sequences. Section 5.1 provides basic results about the linear complexity of sequences. Section 5.2 is devoted to bounds on the weight complexities of binary sequences with **period** $2\sp n$. Due to the importance of ML-sequences in stream **ciphers** , lower bounds on them are developed in Section 5.3. Based on the results of Section 5.3, Section 5.4 cultivates lower bounds on the linear complexities of nonlinear-filtered ML-sequences. Since clock-controlled ML-sequences have their merits as **key** streams, Section 5.5 **develops** bounds on the linear complexities of these sequences. Based on the merits of both clock controlled and nonlinear-filtered binary ML-sequences, a new kind of **key** -stream **generator** is presented, and a lower bound on the linear complexity of the clock-controlled ML-sequences is derived. Because the linear-complexity stability of sequences is of great importance, Section 5.7 provides another approach to it by introducing another two measure **indexes** , i.e., the fixed-complexity distance (FCD) and variable-complexity distance (VCD). Furthermore, the relationship between weight complexity and FCD as well as sphere complexity and VCD is established by using Blahut's theorem. Bounds on the FCD of binary sequences with **period** $2\sp n$ are also developed in this section.

``Chapter 6 discusses the **period** stability of sequences, since the linear complexity stability of sequences has strong connections with their **period** stability. Section 6.1 provides general results about the order of polynomials and that of the **period** of sequences. Section 6.2 first gives, from the viewpoint of stream **ciphers** , two measure **indexes** on the **period** stability of sequences, i.e., weight **period** and sphere **period** . Then it develops the relationship between weight **period** and weight complexity as well as sphere **period** and sphere complexity. Section 6.3 discusses some links between weight **period** and the autocorrelation functions of **periodic** sequences. Sections 6.4 and 6.5 are devoted to the development of some bounds on the weight **period** of some kinds of sequences. Chapter 7 first summarizes the monograph and presents nine open problems of the stability of stream **ciphers** , then introduces the concept and proposes some problems of the stability of source coding for the sources of binary additive stream **ciphers** .

``We would like to make it clear that by the stability of stream **ciphers** , we take its narrow senses to mean the linear-complexity stability and **period** stability as well as the stability of their combining or filtering functions and their source codes. There may be some other **indexes** on the security or strength of stream **ciphers** , whose stabilities need to be investigated.''

Reviewer: From the introduction

Review Type: Abstract

Descriptors: *94A60 -Information and communication, circuits-Communication, information- **Cryptography** (See also 11T71, 68P25) ; 68P25 -Computer science (For papers involving machine computations and programs in a specific mathematical area, see Section --04 in that area)-Theory of data -Data **encryption** (See also 94A60)

13/5/8 (Item 5 from file: 239)

DIALOG(R)File 239:Mathsci

01753445 MR 84i#15001

Counting matrices by Drazin index .

Brawley, J. V.

SIAM J. Algebraic Discrete Methods

Society for Industrial and Applied Mathematics. Journal on Algebraic and Discrete Methods, 1982, 3, no. 1, 30--34. ISSN: 0196-5212 CODEN: SJAMDU

Language: English

Document Type: Journal

Journal Announcement: 1411

Subfile: MR (Mathematical Reviews) AMS

Abstract Length: LONG (31 lines)

Let (F{sub}q){sub}n denote the algebra of n{ **times** }n matrices over F{sub}q, the finite field of q elements, and for each A{in}(F{sub}q){sub}n, let Ind(A) denote the Drazin **index** of A: i.e., Ind(A) is the least nonnegative integer k such that the system of matrix equations (i) A {sup}(k+1)X=A{sup}k, (ii) XAX=X and (iii) AX=XA has a (necessarily unique) solution. The matrix X is called the Drazin inverse of A [M. P. Drazin, Amer. Math. Monthly 65 (1958), 506 - 514; MR 20#5217]. Recently R. E. Hartwig [``Drazin inverses in crytography'', to appear] and J. Levine and Hartwig [**Cryptologia** 4 (1980), 71 - 85; MR 81d:94028] have applied the concept of the Drazin inverse for matrices over finite fields and residue class rings of integers to the Hill **cryptographic** system. Because of this application, Hartwig had asked in a private communication to the author for the number of matrices in (F{sub}q){sub}n that have group inverses, i.e., that are members of some multiplicative group (within the multiplicative semigroup (F{sub}q) {sub}n). It can be shown [see S. L. Campbell and C. B. Meyer Jr., Generalized inverses of linear transformations, Pitman, London, 1979; MR 80d:15003] that the set of matrices in (F{sub}q){sub}n with group inverses is the set of matrices A{in}(F{sub}q){sub}n with Ind(A) <= 1. In the present paper the author determines, for each 0 <= k <= n, the number of A{in}(F{sub}q){sub}n with Ind(A)=k. The sum of these numbers for k=0 and 1 gives the number sought by Hartwig. The **key** to the **determination** is the fact that Ind(A)=k, for

k >= 1, is equal to the **index** of nilpotency of a certain t{ **times** }t nilpotent matrix N, 1 <= t <= n, where A is similar to a matrix diag(B, N) with B invertible. The author extends his results to cover a more general class of finite rings that includes the residue class rings of integers.

```
File 347:JAPIO Nov 1976-2004/Mar(Updated 040708)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200444
         (c) 2004  Thomson Derwent

Set     Items   Description
S1       1389   (SESSION OR INTERVAL OR PERIOD? OR PHASE OR TIME()(BASED OR
                  DEPENDENT) OR TIMEBASED OR INSTANCE OR INSTANT OR CYCLE)(2W)-
                 KEY? ?
S2        358   S1(5N)(ESTABLISH? OR GENERAT? OR CREAT???? OR FASHION? OR -
                 CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR PRODUC?????
                  OR DEVELOP? OR BUILT OR BUILD?)
S3         77   S1(5N)(COMPUTE OR COMPUTES OR COMPUTED OR COMPUTING OR DET-
                 ERMIN? OR DISCERN? OR DERIV? OR CALCULA?)
S4          1   (ITERAT? OR PROGRESSIV?)(5N)S2:S3
S5      26381   KEY? ?(5N)(ESTABLISH? OR GENERAT? OR CREAT???? OR FASHION?
                 OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR PRODUC?-
                 ???? OR DEVELOP? OR BUILT OR BUILD?)
S6       5775   KEY? ?(5N)(COMPUTE OR COMPUTES OR COMPUTED OR COMPUTING OR
                 DETERMIN? OR DISCERN? OR DERIV? OR CALCULA?)
S7         15   (ITERAT? OR PROGRESSIV?)(5N)S5:S6
S8         14   S7 NOT S4
S9          2   (REPEAT? OR REPETITION OR REITERAT?)(5N)S2:S3
S10       127   (REPEAT? OR REPETITION OR REITERAT?)(5N)S5:S6
S11       128   S9:S10
S12       127   S11 NOT S8
S13        21   S12 AND (CRYPTO? OR CRYPTANALY? OR CIPHER? OR CYPHER? OR E-
                 NCRYPT? OR ENCIPHER? OR SCRAMBL? OR DECRYPT? OR DECIPHER? OR -
                 UNENCRYPT? OR UNSCRAMBL?)
S14        20   S13 NOT (S7 OR S9)
S15      3299   (NEXT OR ANOTHER OR SUBSEQUENT? OR SUCCEEDING OR SUCCESSIV?
                  OR FOLLOWING OR ENSU??? OR CONSECUTIV?)(3W)KEY? ?
S16       234   S15(5N)(ESTABLISH? OR GENERAT? OR CREAT???? OR FASHION? OR
                 CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR PRODUC?????
                  OR DEVELOP? OR BUILT OR BUILD?)
S17        58   S15(5N)(COMPUTE OR COMPUTES OR COMPUTED OR COMPUTING OR DE-
                 TERMIN? OR DISCERN? OR DERIV? OR CALCULA?)
S18        88   S16:S17 AND (CRYPTO? OR CRYPTANALY? OR CIPHER? OR CYPHER? -
                 OR ENCRYPT? OR ENCIPHER? OR SCRAMBL? OR DECRYPT? OR DECIPHER?
                 OR UNENCRYPT? OR UNSCRAMBL?)
S19        87   S18 NOT (S7 OR S9 OR S14)
S20        29   S19 AND AC=US/PR
S21        24   S20 AND AY=(1965:2001)/PR
S22        53   S19 AND PY=1965:2001
S23        61   S21:S22
S24        14   S23 AND PUBLIC()KEY? ?
S25      1369   (COMMON OR SHARED)(2W)KEY? ?
S26         2   S24 AND S25
S27        47   S23 NOT (S24 OR S26)
S28        11   S27 AND TIME
S29        36   S27 NOT S28
S30       261   (INTERVAL? ? OR PERIOD? OR TIME) AND S25
S31       159   S30 AND (CRYPTO? OR CRYPTANALY? OR CIPHER? OR CYPHER? OR E-
                 NCRYPT? OR ENCIPHER? OR SCRAMBL? OR DECRYPT? OR DECIPHER? OR -
                 UNENCRYPT? OR UNSCRAMBL?)
S32        29   S31 AND (TIMES OR PERIOD? OR INTERVAL? ?)
S33        28   S32 NOT (S7 OR S9 OR S14 OR S24 OR S26 OR S28)
S34         0   S29 AND (INDEX OR INDEXES OR INDICES OR KEY()SCHEDULE? ?)
S35       669   S5:S6 AND S25
S36       511   S35 AND (CRYPTO? OR CRYPTANALY? OR CIPHER? OR CYPHER? OR E-
                 NCRYPT? OR ENCIPHER? OR SCRAMBL? OR DECRYPT? OR DECIPHER? OR -
                 UNENCRYPT? OR UNSCRAMBL?)
S37        87   S36 AND (TIME OR PERIOD? OR INTERVAL? ?)
S38        72   S37 NOT (S7 OR S9 OR S14 OR S24 OR S26 OR S28 OR S29 OR S3-
                 3)
S39         3   S38 AND (INDEX OR INDEXES OR INDICES OR KEY()SCHEDULE? ?)
S40        14   S37 AND (TIMES OR PERIOD? OR INTERVAL? ?)
S41         0   S40 NOT (S7 OR S9 OR S14 OR S24 OR S26 OR S28 OR S29 OR S3-
```

14/5/19 (Item 16 from file: 350)
DIALOG(R)File 350:Derwent WPIX

007527533 **Image available**
WPI Acc No: 1988-161465/198823
XRPX Acc No: N88-123315

Encrypted **information processing system for software security - has output key used by** decrypter **generator produced in microprocessor hardware according to inaccessible algorithm**

Patent Assignee: TAAFFE J L (TAAF-I)
Inventor: TAAFFE J L
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 4747139	A	19880524	US 86921851	A	19861021	198823	B

Priority Applications (No Type Date): US 84644556 A 19840827; US 86921851 A 19861021

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 4747139	A		11		

Abstract (Basic): US 4747139 A

The **encrypted** information processing system key generator hardware for processing an input key associated with the **encrypted** information according to an algorithm to generate a unique output key. The **decryption** key generator uses a single chip microprocessor programmed as a finite state machine which, in each of several states, responds to a predetermined input word to change to another state and output a corresponding output key word. A number of **repeatable** output **key** word sequences are **generated** only with predetermined input **key** word sequences, each word of a repeatable output sequence being dependent on both the present state of the microprocessor and on an input word to the microprocessor which is acceptable at that state.

A **decrypter** for receives the **encrypted** information and a corresponding output key from the klekey generator hardware to **decrypt** the received **encrypted** information based on the received output key.

USE/ADVANTAGE - For protecting software from unauthorised access and copying number of possible inputs to key generator is very large

Title Terms: **ENCRYPTION** ; INFORMATION; PROCESS; SYSTEM; SOFTWARE; SECURE; OUTPUT; KEY; **DECRYPTER** ; GENERATOR; PRODUCE; MICROPROCESSOR; HARDWARE; ACCORD; INACCESSIBLE; ALGORITHM
Derwent Class: T01; W01
International Patent Class (Additional): H04L-009/00
File Segment: EPI

14/5/20 (Item 17 from file: 350)
DIALOG(R)File 350:Derwent WPIX

007031405
WPI Acc No: 1987-031402/198705
XRPX Acc No: N87-023719

Television scrambler **with electronic variable key - has key validation signal transmitted to receivers along with key containing rank identifying data**

Patent Assignee: CNET ETAT FR PTT TE (ETFR); TELEDIFFUSION DE FRANCE (TELG)
Inventor: CHRISTIAN J F G
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
FR 2583946	A	19861226	FR 859679	A	19850624	198705	B

Priority Applications (No Type Date): FR 859679 A 19850624

Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
FR 2583946 A 23

Abstract (Basic): FR 2583946 A

A variable electronic key **scrambles** the information at the transmitter and **unscrambles** it at the receiver, the key being transmitted in any known fashion, as well as the key, a signal for validating the key is transmitted from the transmitter to the receivers.

Pref., the different keys contain an item of information which identifies their ranks or levels, each validation signal also containing the same item of information allowing the identification of the key used. Each key is determined in the receiver from a transmitter- **produced** message and a subscriber **key** **repeated** at regular intervals.

USE/ADVANTAGE - Teletext systems. Accounts for noise.

0/9

Title Terms: TELEVISION; **SCRAMBLE** ; ELECTRONIC; VARIABLE; KEY; KEY; VALID; SIGNAL; TRANSMIT; RECEIVE; KEY; CONTAIN; RANK; IDENTIFY; DATA

Index Terms/Additional Words: TELETEXT

Derwent Class: W02

International Patent Class (Additional): H04N-007/16

File Segment: EPI

28/5/6 **(Item 2 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

[illegible]105820 **Image available**
WPI Acc No: 2000-277691/ **200024**
XRPX Acc No: N00-209034
Key management method for encryption **communication system, involves generating session key and disclosure key using common key and** time **information**
Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2000075788	A	20000314	JP 98247452	A	1998090	200024	B

Priority Applications (No Type Date): JP 98247452 A 19980901
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2000075788	A		14	G09C-001/00	

Abstract (Basic): JP 2000075788 A

NOVELTY - Session and disclosure keys are generated using common key and **time** information. The **time** information is **encrypted** by session key and is considered as execution consent information. The session key belongs to key storage group which is in lower order from secret key of transmission side user apparatus, while the disclosure key belongs to higher order group from that of the receiver side user apparatus.

DETAILED DESCRIPTION - When the **next** session **key** is **generated** and there is no group in lower order from the execution consent information, the secret key of the transmission side user apparatus, the common key which consists of disclosure key of receiving side user apparatus and the **time** information are transmitted to the receiving side user apparatus and the message is **encrypted** using the session key. Appending information which includes **time** information is generated and is transmitted to the receiving side user apparatus.

INDEPENDENT CLAIMS are also included for the following:

(a) key management method;

(b) key management apparatus;

(c) program for key management

USE - For **encryption** communication system.

ADVANTAGE - The number of system T required for decoding in each hierarchy can be set-up independently. Comparison of appending information is not needed at the receiving side.

pp; 14 DwgNo 1/13

Title Terms: KEY; MANAGEMENT; METHOD; **ENCRYPTION** ; COMMUNICATE; SYSTEM; GENERATE; SESSION; KEY; DISCLOSE; KEY; COMMON; KEY; **TIME** ; INFORMATION
Derwent Class: P85; W01
International Patent Class (Main): G09C-001/00
International Patent Class (Additional): H04L-009/08
File Segment: EPI; EngPI

28/5/7 **(Item 3 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

[illegible]12659037 **Image available**
WPI Acc No: 2000-030870/ **200003**
XRPX Acc No: N00-023894
Encryption **key generator of storage type broadcast reception apparatus for communication system - generates independent** encryption **keys for viewing and listening to real** time **and stored program data respectively which has been transmitted**
Patent Assignee: MATSUSHITA DENKI SANGYO KK (MATU)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 11298874	A	19991029	JP 98208909	A	19980724	200003	B

Priority Applications (No Type Date): JP 9832463 A 19980216

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 11298874	A		56	H04N-007/16	

Abstract (Basic): JP 11298874 A

NOVELTY - An **encryption** key is generated by generator (206) for real **time** viewing and listening of program data simultaneously while program is being transmitted. The transmitted program is stored. **Another** storage **encryption** **key** is independently **generated** for viewing and listening of stored program data in future.

USE - For communication system.

ADVANTAGE - By using different **encryption** keys to **encrypt** the program while storing and transmitting, the program is protected effectively from unauthorized viewers. DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the storage type broadcast reception apparatus. (206) Generator.

Dwg.1/31

Title Terms: **ENCRYPTION** ; KEY; GENERATOR; STORAGE; TYPE; BROADCAST; RECEPTION; APPARATUS; COMMUNICATE; SYSTEM; GENERATE; INDEPENDENT; **ENCRYPTION** ; KEY; VIEW; LISTENER; REAL; **TIME** ; STORAGE; PROGRAM; DATA; RESPECTIVE; TRANSMIT

29/5/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO

05720156 **Image available**
CIPHERING METHOD AND DEVICE THEREFOR, RECORDING METHOD, DECODING METHOD AND DEVICE THEREFOR AND RECORDING MEDIUM

PUB. NO.: 10-003256 [JP 10003256 A]
PUBLISHED: January 06, 1998 (**19980106)**
INVENTOR(s): ISHIGURO RYUJI
APPLICANT(s): SONY CORP [000218] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-269502 [JP 96269502]
FILED: October 11, 1996 (19961011)
INTL CLASS: [6] G09C-001/00; G09C-001/00; G09C-001/00; G11B-020/10; H04L-009/08; H04L-009/06; H04L-009/14
JAPIO CLASS: 44.9 (COMMUNICATION -- Other); 42.5 (ELECTRONICS -- Equipment); 44.3 (COMMUNICATION -- Telegraphy)
JAPIO KEYWORD:R009 (HOLOGRAPHY); R102 (APPLIED ELECTRONICS -- Video Disk Recorders, VDR); R107 (INFORMATION PROCESSING -- OCR & OMR Optical Readers); R138 (APPLIED ELECTRONICS -- Vertical Magnetic & Photomagnetic Recording)

ABSTRACT
PROBLEM TO BE SOLVED: To easily control the **ciphering** key.

SOLUTION: A **ciphering** key K1 is generated from a master key K0 using a unidirectional function, a **next ciphering key** K2 is **generated** from the key K1 using the function and similarly n-hierarchial **ciphering** keys K1 to Kn are generated. Then, information is **ciphered** by the key Kn and the information is decoded by the **ciphering** key Kn. If the key Kn is read, the information is **ciphered** by the key Kn-1 and the information is decoded by the key Kn-1. Thus, the information, which is **ciphered** by the key Kn, is decoded by the key Kn obtained from the key Kn-1 using the function and the user is only required to maintain the latest key Kn-1.

29/5/3 (Item 3 from file: 347)
DIALOG(R)File 347:JAPIO

02226636 **Image available**
INTER-LINE **CIPHER** DEVICE COMMUNICATION SYSTEM

PUB. NO.: 62-143536 [JP 62143536 A]
PUBLISHED: June 26, 1987 (**19870626)**
INVENTOR(s): MIYOSHI HIROYUKI
NAKAI TOSHIHISA
APPLICANT(s): OKI ELECTRIC IND CO LTD [000029] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 60-283038 [JP 85283038]
FILED: December 18, 1985 (19851218)
INTL CLASS: [4] H04L-009/02
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy)
JOURNAL: Section: E, Section No. 563, Vol. 11, No. 376, Pg. 28, December 08, 1987 (19871208)

ABSTRACT
PURPOSE: To reduce the volume of data to be transferred by constituting a species data, a data key **enciphered** with a master key, and a master key authorizing data **enciphered** with the data key as a telegram having a communication frame format.

CONSTITUTION: A CPU11 at a line **cipher** device 42 generates species data of two bytes SV1 and SV2 with a random number generation algorithm, furthermore, the data is expanded to an initial value data of eight bytes with a common algorithm at line **cipher** devices 42 and 46. **Next** , a data

key K is **generated** with the random number algorithm, and the data key is **enciphered** with a CIP13 based on a master key KM and the initial value data set manually in advance at an SW14 in the line **cipher** device 42 using the **cipher** feed back mode of a DES algorithm, and an EKMK (eight bytes) can be obtained. Furthermore, an authorizing data CKCD is similarly **enciphered** with the data key K, and an EK(CKCD) can be obtained. The communication frame format is generated using the data generated with the above processing.

29/5/4 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015095541 **Image available**
WPI Acc No: 2003-156059/200315
XRPX Acc No: N03-123156
Secured information exchange method for business application, involves determining subsequent encryption key **using** decrypted **information and private key**
Patent Assignee: DISANTO F J (DISA-I); KRUSOS D A (KRUS-I)
Inventor: DISANTO F J; KRUSOS D A
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020150237	A1	20021017	US 2001782825	A	20010214	200315	B

Priority Applications (No Type Date): US 2001782825 A 20010214
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020150237	A1		15	H04L-009/00	

Abstract (Basic): US 20020150237 A1

NOVELTY - The information set is **encrypted** using an **encryption** key determined from the information set that is previously exchanged between the terminals (100,110). The received **encrypted** information set is **decrypted** using prestored private key. corresponding to an information set is **determined** and stored. The **next** **encryption** **key** is **determined** using the **decrypted** information and private key.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

(1) Information exchange system; and

(2) Information exchange device.

USE - For securely exchanging information like business strategy, credit card numbers, social security number, bank account balances, medical record, etc., between terminals using communication network.

ADVANTAGE - By **determining** the **subsequent** **encryption** **key** using the **decrypted** information and the private key, the information are efficiently and securely exchanged between the terminals.

DESCRIPTION OF DRAWING(S) - The figure shows the schematic view of the information exchange system.

Terminals (100,110)

pp; 15 DwgNo 3/7

Title Terms: SECURE; INFORMATION; EXCHANGE; METHOD; BUSINESS; APPLY; DETERMINE; SUBSEQUENT; **ENCRYPTION** ; KEY; INFORMATION; PRIVATE; KEY
Derwent Class: T01; T05; W01
International Patent Class (Main): H04L-009/00
File Segment: EPI

29/5/5 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015086701 **Image available**
WPI Acc No: 2003-147219/200314
Related WPI Acc No: 2003-711858
XRPX Acc No: N03-116218

Object securing method in cryptographic data securing system, involves adding object which is encrypted using working split formed by combining splits including random key components, with header
Patent Assignee: TECSEC INC (TECS-N)
Inventor: DOMANGUE E L; SCHEIDT E M
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6490680	B1	20021203	US 9768785	P	19971204	200314	B
			US 98205221	A	19981204		

Priority Applications (No Type Date): US 9768785 P 19971204; US 98205221 A 19981204
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6490680	B1		17	H04L-009/00	Provisional application US 9768785

Abstract (Basic): US 6490680 B1

NOVELTY - Several splits including random key components are combined to form a working split, using which the object is **encrypted** . **Another** splits without random **key** components are combined to **form** a value, using which random key component is **encrypted** . A header formed with information containing user algorithm, **encrypted** key component and **decrypt** read credentials, is **encrypted** and added to the **encrypted** object.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for object **decryption** method.

USE - For objects securing in **cryptographic** data security system for communication system and communication network such as LAN and WAN.

ADVANTAGE - Enables flexible access for authorized users of the communication system, while maintaining security for stored data and data being transmitted.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of key **encryption** process using digital signature.

pp; 17 DwgNo 1/6

Title Terms: OBJECT; SECURE; METHOD; **CRYPTOGRAPHIC** ; DATA; SECURE; SYSTEM; ADD; OBJECT; **ENCRYPTION** ; WORK; SPLIT; FORMING; COMBINATION; SPLIT; RANDOM; KEY; COMPONENT; HEADER
Derwent Class: T01; W01
International Patent Class (Main): H04L-009/00
International Patent Class (Additional): H04L-009/30
File Segment: EPI

29/5/6 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014769015 **Image available**
WPI Acc No: 2002-589719/200263
XRPX Acc No: N02-467962

Asymmetric crypto -key generation system for crypto systems, has processor which divides private crypto -key into two portion and deletes private crypto -key and key portion associated with user's password without storing them

Patent Assignee: DESA C (DESA-I); GANESAN K (GANE-I); SANDHU R (SAND-I); SINGLESIGNON.NET (SING-N)
Inventor: DESA C; GANESAN K; SANDHU R
Number of Countries: 021 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020076042	A1	20020620	US 2000739260	A	20001219	200263	B
WO 200251062	A1	20020627	WO 2001US48203	A	20011218	200263	

Priority Applications (No Type Date): US 2000739260 A 20001219
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020076042	A1		29	H04L-009/00	

WO 200251062 A1 E H04L-009/00
Designated States (National): JP
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

Abstract (Basic): US 20020076042 A1

NOVELTY - A processor generates private **crypto** -key and corresponding public **crypto** -key. The private **crypto** -key is divided into two portions, among which one portion is based on user's password. The private **crypto** -key and user's password-based key portion are deleted without storage, whereas the public **crypto** -key and other key portion are stored in a memory persistently. **Another** processor **generates** a **key** portion with an one-way function, when the same user's password is received, and then deletes the generated portion without storing.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

(1) Transformed message communication system;
(2) Asymmetric **crypto** -key generation method; and
(3) Transformed message communication method.

USE - Asymmetric **crypto** -key generation system for **crypto** systems.

ADVANTAGE - Asymmetric **crypto** -keys provide trusted authentication of user to other users, as the private **crypto** -key and user password-based key portion are deleted without storing. Enables users to manage their information in a secure manner by deleting, changing or modifying the information.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart explaining the operation carried out by a user, distinguished server and sponsor station in associating asymmetric key pair with the user.

pp; 29 DwgNo 6a/11

Title Terms: ASYMMETRIC; KEY; GENERATE; SYSTEM; SYSTEM; PROCESSOR; DIVIDE; PRIVATE; KEY; TWO; PORTION; DELETE; PRIVATE; KEY; KEY; PORTION; ASSOCIATE ; USER; PASSWORD; STORAGE
Derwent Class: T01; W01
International Patent Class (Main): H04L-009/00
File Segment: EPI

29/5/7 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014584036 **Image available**
WPI Acc No: 2002-404740/200243
XRPX Acc No: N02-317729

Cryptographic **key establishment method for** cryptographic **system, involves computing session key using public quantities transmitted between sender and receiver**

Patent Assignee: CHANG C N (CHAN-I)
Inventor: CHANG C N
Number of Countries: 095 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200221765	A1	20020314	WO 2001US27148	A	20010831	200243	B
AU 200190594	A	20020322	AU 200190594	A	20010831	200251	

Priority Applications (No Type Date): US 2000655229 A 20000905
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200221765	A1	E	27	H04L-009/30	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200190594 A H04L-009/30 Based on patent WO 200221765

Abstract (Basic): WO 200221765 A1

NOVELTY - Public quantities transmitted by receiver (12b) for storage in a public repository (67), are retrieved by a sender (12a). Sender's quantities and session key (R) are computed using the public quantities by the sender and transmitted to the receiver, for computing **another** session **key** (K) and received quantities.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) **Cryptographic** system;

(b) **Cryptographic** unit

USE - For establishing **cryptographic** key between sender and receiver for exchanging **encrypted** **cyphertext** messages in **cryptographic** system (claimed) using communication channels such as telephone link, radio link, microwave link, fiber optic link and coaxial cable link.

ADVANTAGE - Enables faster and secure exchange of **cryptographic** key between sending and receiving **cryptographic** units.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the **cryptographic** system.

Sender (12a)

Receiver (12b)

Public repository (67)

Session keys (K,R)

pp; 27 DwgNo 1/1

Title Terms: **CRYPTOGRAPHIC** ; KEY; ESTABLISH; METHOD; **CRYPTOGRAPHIC** ; SYSTEM; COMPUTATION; SESSION; KEY; PUBLIC; QUANTITY; TRANSMIT; SEND; RECEIVE

Derwent Class: W01

International Patent Class (Main): H04L-009/30

File Segment: EPI

29/5/8 (Item 5 from file: 350)

DIALOG(R)File 350:Derwent WPIX

014453943 **Image available**

WPI Acc No: 2002-274646/ **200232**

XRPX Acc No: N02-214301

Authentication method for network connected terminal, involves generating common key using confidential information corresponding to model number of terminal

Patent Assignee: MATSUSHITA DENKI SANGYO KK (MATU)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2001344214	A	20011214	JP 2000163226	A	20000531	200232	B

Priority Applications (No Type Date): JP 2000163226 A 20000531

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2001344214	A		18	G06F-015/00	

Abstract (Basic): JP 2001344214 A

NOVELTY - A common key is generated using the confidential information corresponding to the model number of a terminal, and is used to **encrypt** the body number of the terminal. **Another** common **key** is **generated** using the confidential information corresponding to the body number, and is used for comparison.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for **encryption** communication system of terminal.

USE - For authenticating terminal connected to network.

ADVANTAGE - Enables maintaining high secrecy property by generating the common key. Eliminates the possibility that terminals other than that having specific model number are connected to the server.

DESCRIPTION OF DRAWING(S) - The figure explains the authentication method. (Drawing includes non-English language text).

pp; 18 DwgNo 1/13
Title Terms: AUTHENTICITY; METHOD; NETWORK; CONNECT; TERMINAL; GENERATE; COMMON; KEY; CONFIDE; INFORMATION; CORRESPOND; MODEL; NUMBER; TERMINAL
Derwent Class: T01; W01
International Patent Class (Main): G06F-015/00
International Patent Class (Additional): G06F-013/00; H04L-009/08; H04L-009/32
File Segment: EPI

29/5/9 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014441273 **Image available**
WPI Acc No: 2002-261976/ **200231**
XRPX Acc No: N02-203573

Content information transmission method e.g. for digital audio-video data, involves encrypting **content information using key obtained based on key information** encrypted **using another key**

Patent Assignee: VICTOR CO OF JAPAN (VICO)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2001274784	A	20011005	JP 200045842	A	20000223	200231	B

Priority Applications (No Type Date): JP 20009902 A 20000119
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2001274784	A		8	H04L-009/08	

Abstract (Basic): JP 2001274784 A

NOVELTY - Content information is **encrypted** using a key obtained based on key information. The key information contains **encrypted** information obtained by **encrypting** key information using **another key** . A transmission **key** with predetermined function is **generated** and transmitted along with the **encrypted** content information.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Content information recording method;
(b) Content information transmission device;
(c) Content information recording device;
(d) Transmission medium;
(e) Recording medium

USE - E.g. for digital audio-video data.

ADVANTAGE - Enables to reproduce **encrypted** content information exactly at the reproduction side and enables reproduction of content information only in normal conditions.

DESCRIPTION OF DRAWING(S) - The figure shows the schematic components of the content information transmission device. (Drawing includes non-English language text).

pp; 8 DwgNo 1/2
Title Terms: CONTENT; INFORMATION; TRANSMISSION; METHOD; DIGITAL; AUDIO; VIDEO; DATA; CONTENT; INFORMATION; KEY; OBTAIN; BASED; KEY; INFORMATION; **ENCRYPTION** ; KEY
Derwent Class: T01; W01; W04
International Patent Class (Main): H04L-009/08
International Patent Class (Additional): G06F-015/00
File Segment: EPI

29/5/10 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014293124 **Image available**
WPI Acc No: 2002-113826/ **200215**
XRPX Acc No: N02-084884

Digital video content transmission ciphering **method involves** generating successive **number of frame** keys **using session key for** ciphering **corresponding frames of multi-frame video content to be transmitted**

Patent Assignee: INTEL CORP (ITLC)
Inventor: FABER R W; GRAUNKE G L; LEE D A
Number of Countries: 096 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200117251	A1	20010308	WO 2000US22785	A	20000817	200215	B
AU 200069184	A	20010326	AU 200069184	A	20000817	200215	
EP 1212893	A1	20020612	EP 2000957587	A	20000817	200239	
			WO 2000US22785	A	20000817		
KR 2002053808	A	20020705	KR 2002702727	A	20020228	200302	
JP 2003508975	W	20030304	WO 2000US22785	A	20000817	200319	
			JP 2001521065	A	20000817		
CN 1385032	A	20021211	CN 2000815064	A	20000817	200324	
TW 501370	A	20020901	TW 2000117509	A	20000829	200334	
US 6731758	B1	20040504	US 99385592	A	19990829	200430	

Priority Applications (No Type Date): US 99385592 A 19990829
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200117251	A1	E	34	H04N-007/167	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
AU 200069184	A				Based on patent WO 200117251
EP 1212893	A1	E		H04N-007/167	Based on patent WO 200117251

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL RO SI

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2002053808	A			H04N-007/167	
JP 2003508975	W		39	H04N-007/167	Based on patent WO 200117251
CN 1385032	A			H04N-007/167	
TW 501370	A			H04N-007/167	
US 6731758	B1			H04N-007/167	

Abstract (Basic): WO 200117251 A1

NOVELTY - A session key is generated for each transmission session within which multi-frame video content is to be transmitted to a video sink device (104) through a digital video link (106). Using the session key, a **successive** number of frame **keys** are **generated** for **ciphering** corresponding frames of the multi-frame video content.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Digital video content transmission **ciphering** apparatus;

(b) Digital video content transmission **deciphering** method

USE - Digital video content transmission **ciphering** method.

ADVANTAGE - Video content is protected from unauthorized copying during transmission, since the frames of the video content are **ciphered** before transmission.

DESCRIPTION OF DRAWING(S) - The figure shows the overview of video content transmission system.

Video sink device (104)

Digital video link (106)

pp; 34 DwgNo 1/8

29/5/18 (Item 15 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013662808 **Image available**
WPI Acc No: 2001-147020/ **200115**
XRPX Acc No: N01-107677

Communications systems method and arrangements for secure linking of entity authentication and ciphering **key generation conducts entity authentication process using** cryptography **key when a cuphering offset value is generated**

Patent Assignee: TELEFONAKTIEBOLAGET ERICSSON L M (TELF)
Inventor: SMEETS B J M; SMEETS B
Number of Countries: 095 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200101630	A1	20010104	WO 2000EP5742	A	20000621	200115	B
AU 200058176	A	20010131	AU 200058176	A	20000621	200124	
BR 200011870	A	20020305	BR 200011870	A	20000621	200225	
			WO 2000EP5742	A	20000621		
EP 1190526	A1	20020327	EP 2000943854	A	20000621	200229	
			WO 2000EP5742	A	20000621		
CN 1371565	A	20020925	CN 2000812025	A	20000621	200305	
JP 2003503896	W	20030128	WO 2000EP5742	A	20000621	200309	
			JP 2001506186	A	20000621		
US 6633979	B1	20031014	US 99344387	A	19990625	200368	

Priority Applications (No Type Date): US 99344387 A 19990625
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200101630	A1	E	22	H04L-009/32	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
AU 200058176	A				Based on patent WO 200101630
BR 200011870	A			H04L-009/32	Based on patent WO 200101630
EP 1190526	A1	E		H04L-009/32	Based on patent WO 200101630

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
CN 1371565	A			H04L-009/32	
JP 2003503896	W		28	H04L-009/08	Based on patent WO 200101630
US 6633979	B1			G06F-001/24	

Abstract (Basic): WO 200101630 A1

NOVELTY - The method uses an authentication pprocess to generate a **ciphering** offset value (50). Each node (12,14) stores offset value and uses it to **generate subsequent ciphering keys** employed to **encrypt** data transmitted between the nodes, so a logical relationship between the latest entity authentication process and **subsequently generated ciphering keys** increasing the security and reduce overheads.

DETAILED DESCRIPTION - Independent claims describe an arrangement for generating **ciphering** keys in a communication node and a system.

USE - As a method and arrangements for secure linking of entity authentication and **ciphering** key generation.

ADVANTAGE - Can enhance security in any communication system including a mobile telecommunications system, for example, a global system for mobile (GSM) communications syatem.

DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram depicting an improved authentication process and arrangement associated with secure communications system, for example.

the **ciphering** offset value (50)

the nodes (12 and 14)

pp; 22 DwgNo 4/7

Title Terms: COMMUNICATE; SYSTEM; METHOD; ARRANGE; SECURE; LINK; ENTITY;

AUTHENTICITY; **CIPHER** ; KEY; GENERATE; CONDUCTING; ENTITY; AUTHENTICITY; PROCESS; KEY; OFFSET; VALUE; GENERATE
Derwent Class: W01; W02
International Patent Class (Main): G06F-001/24; H04L-009/08; H04L-009/32
International Patent Class (Additional): H04Q-007/38
File Segment: EPI

29/5/19 (Item 16 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013647898 **Image available**
WPI Acc No: 2001-132107/ **200114**
XRPX Acc No: N01-098202
Encryption **communication system, has key determining unit which determines** encrypting **key used by transmitting station and decoding key used by receiving station via transfer of discriminative data**
Patent Assignee: MITSUBISHI ELECTRIC CORP (MITQ)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2000358022	A	20001226	JP 99168845	A	19990615	200114	B

Priority Applications (No Type Date): JP 99168845 A 19990615
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2000358022	A		8	H04L-009/08	

Abstract (Basic): JP 2000358022 A

NOVELTY - The discriminative information uniquely specifying the **encryption** key is stored and subsequently matched with an **encryption** key into a memory unit. The **encryption** key used by a transmitting station and the decoding key used by a receiving station is determined by a key determining unit through the transfer of the stored discriminative information.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) an **encryption** key determining method;

(b) a recording medium into which the computer program in determining the **encryption** key is recorded

USE - For computer network.

ADVANTAGE - **Ensures** that **encryption key** can be **determined** quickly and efficiently. Prevents leakage of data to an unauthorized **encrypting** apparatus.

DESCRIPTION OF DRAWING(S) - The figure shows the functional block diagram of the system assembly of the **encryption** communication system.

pp; 8 DwgNo 1/6
Title Terms: **ENCRYPTION** ; COMMUNICATE; SYSTEM; KEY; DETERMINE; UNIT; DETERMINE; KEY; TRANSMIT; STATION; DECODE; KEY; RECEIVE; STATION; TRANSFER; DISCRIMINATE; DATA
Derwent Class: W01
International Patent Class (Main): H04L-009/08
File Segment: EPI

29/5/20 (Item 17 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013474347 **Image available**
WPI Acc No: 2000-646290/ **200062**
XRPX Acc No: N00-478894
Digitally signing method for specified document in financial transactions, involves generating digital signature for specified document as predefined function of private key, document digest and pseudo-random key

Patent Assignee: AGORICS INC (AGOR-N)
Inventor: HARDY N; TRIBBLE E D; VETTER L L
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6079018	A	20000620	US 97947375	A	19971008	200062	B

Priority Applications (No Type Date): US 97947375 A 19971008
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6079018	A		16	H04L-009/20	

Abstract (Basic): US 6079018 A

NOVELTY - Private key associated with person or entity signing document are received. Digest of specified document is output by predefined one-way hash function. A digital signature is generated for specified document as predefined function of private key, document digest and pseudo-random key (k). A distinct pseudo random key is generated for each distinct specified document.

DETAILED DESCRIPTION - Pseudo random key **generation** includes the **following** steps. The private **key** is hashed with the predefined one-way hash function to generate an intermediate value. The document digest is combined with a value corresponding to the intermediate value and an ancillary secret value to generate another intermediate value which is then hashed with the predefined one-way has function to generate pseudo-random key (k) by predefined computational technique. For the given private key, distinct digital signature is generated for each distinct specified document. INDEPENDENT CLAIMS are also included for the following:

(a) digital signing program stored in recording medium;

(b) digital signing system for specified document

USE - For digitally signing specified documents in electronic transactions such as financial transactions for providing security features. Financial services technology consortium (FSTC) electronic check (E-check) project utilize the digital signature standard for signing computerized documents such as E-checks. DSS uses the public digital signature algorithm (DSA) to compute various **encryption** key components and supply a digital signature to each signed component.

ADVANTAGE - Eliminates the key exposure problem generated due to multiple smart cards for the same user key using simple technique. Highly unguessable pseudo-random key seed value is generated reliably. Facilitates to perform special computations that entirely eliminate the danger of signing different documents with the same pseudo-random key value.

DESCRIPTION OF DRAWING(S) - The figure shows the data flow diagram of computer system.

pp; 16 DwgNo 3/6

Title Terms: DIGITAL; SIGN; METHOD; SPECIFIED; DOCUMENT; FINANCIAL; TRANSACTION; GENERATE; DIGITAL; SIGNATURE; SPECIFIED; DOCUMENT; PREDEFINED; FUNCTION; PRIVATE; KEY; DOCUMENT; DIGEST; PSEUDO; RANDOM; KEY
Derwent Class: W01
International Patent Class (Main): H04L-009/20
File Segment: EPI

29/5/21 (Item 18 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013378853 **Image available**
WPI Acc No: 2000-550791/ **200051**
XRPX Acc No: N00-407467

Authentication system for establishing telephone calls includes exchange of data via operator, and subsequent determination **of encoded** key

Patent Assignee: SOC FR DU RADIOTELEPHONE (FRRA-N); SFR SOC FR RADIOTELEPHONE SA (SFRF-N)
Inventor: WARY J M; WARY J P; WARY M J
Number of Countries: 027 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1022922	A1	20000726	EP 2000460005	A	20000121	200051	B
FR 2788914	A1	20000728	FR 99901	A	19990122	200051	
JP 2000232690	A	20000822	JP 200014375	A	20000124	200055	
US 6745326	B1	20040601	US 2000489952	A	20000124	200436	

Priority Applications (No Type Date): FR 99901 A 19990122

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1022922	A1	F	15	H04Q-007/38	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
FR 2788914	A1			H04L-009/32	
JP 2000232690	A		11	H04Q-007/38	
US 6745326	B1			H04L-009/00	

Abstract (Basic): EP 1022922 A1

NOVELTY - The system includes an initial inscription process, followed by an exchange of authentication data

DETAILED DESCRIPTION - The process provides authentication of a subscriber and establishment of a secure connection channel between a subscriber and a service provider. It includes an initial inscription process when the subscriber communicates with the service provider via the operator. The process includes an exchange of authentication data (DeviceID, R1; login, mdp) on line and off line. The encoded channel is eventually established at the start of each session, after mutual authentication, which also uses **cryptographic** functions. Finally an encoding key (Kses) is established without transmission of a secret element on the network(s).

USE - Connection of mobile telephone to network.

ADVANTAGE - Facilitates secure connection over GSM telephone system.

DESCRIPTION OF DRAWING(S) - The figure shows the sequence of establishing the communication channel.

pp; 15 DwgNo 2/3

Title Terms: AUTHENTICITY; SYSTEM; ESTABLISH; TELEPHONE; CALL; EXCHANGE; DATA; OPERATE; SUBSEQUENT; DETERMINE; ENCODE; KEY

Derwent Class: W01; W02

International Patent Class (Main): H04L-009/00; H04L-009/32; H04Q-007/38

International Patent Class (Additional): H04M-001/66; H04Q-007/20; H04Q-007/22; H04Q-007/24; H04Q-007/26; H04Q-007/30

File Segment: EPI

29/5/22 (Item 19 from file: 350)

DIALOG(R)File 350:Derwent WPIX

013291761 **Image available**

WPI Acc No: 2000-463696/ 200040

XRPX Acc No: N00-345867

Program material decryption **for digital CATV system, involves sending key initially to** decrypt **specific program while** following key produces **initially sent key from** cipher **text and** decrypts **specific program**

Patent Assignee: LUCENT TECHNOLOGIES INC (LUCE)

Inventor: RICHARDS W J

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6069957	A	20000530	US 97810441	A	19970307	200040	B

Priority Applications (No Type Date): US 97810441 A 19970307

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6069957	A		42	H04L-009/00	

Abstract (Basic): US 6069957 A

NOVELTY - A certain key is transmitted initially to **decrypt** program A. A specific key is transmitted following which produces the initially sent key from **cipher** text and **decrypts** program B.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for program material **decryption** system.

USE - For digital cable television system, video conferencing system.

ADVANTAGE - The present **decryption** method suits the unique capabilities of digital signal transmission.

DESCRIPTION OF DRAWING(S) - The figure shows the explanation of **encryption** of program.

pp; 42 DwgNo 25/31

Title Terms: PROGRAM; MATERIAL; **DECRYPTER** ; DIGITAL; CATV; SYSTEM; SEND; KEY; INITIAL; SPECIFIC; PROGRAM; FOLLOW; KEY; PRODUCE; INITIAL; SEND; KEY ; **CIPHER** ; TEXT; SPECIFIC; PROGRAM

Derwent Class: W01; W02

International Patent Class (Main): H04L-009/00

International Patent Class (Additional): H04K-001/00

File Segment: EPI

29/5/23 (Item 20 from file: 350)

DIALOG(R)File 350:Derwent WPIX

012915319 **Image available**

WPI Acc No: 2000-087155/ 200007

XRPX Acc No: N00-068421

Password creating method for controlling usage of software component

Patent Assignee: INTEL CORP (ITLC)

Inventor: KNAPTON K S

Number of Countries: 086 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9963707	A1	19991209	WO 99US11106	A	19990519	200007	B
AU 9940054	A	19991220	AU 9940054	A	19990519	200021	
EP 1084549	A1	20010321	EP 99923231	A	19990519	200117	
			WO 99US11106	A	19990519		
US 6363486	B1	20020326	US 9892632	A	19980605	200226	

Priority Applications (No Type Date): US 9892632 A 19980605

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9963707	A1	E	29	H04L-009/32	

Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
AU 9940054	A			H04L-009/32	Based on patent WO 9963707
EP 1084549	A1	E		H04L-009/32	Based on patent WO 9963707

Designated States (Regional): DE FR GB

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6363486	B1			H04L-009/00	

Abstract (Basic): WO 9963707 A1

NOVELTY - A secret **encryption** key is created corresponding to identifier of application program. **Another** secret **encryption key** is **created** corresponding to identifier of component. Based on the created secret **encryption** keys, a password for controlling usage of software component, is created.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) article comprising machine readable storage medium;

(b) user computer system

USE - For controlling usage of software component.

ADVANTAGE - Ensures that a component functions only with the

application program, has license number, thus secures capability for plug-in or snap-in of component.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of operating environment.

pp; 29 DwgNo 1/5

Title Terms: PASSWORD; METHOD; CONTROL; SOFTWARE; COMPONENT
Derwent Class: W01
International Patent Class (Main): H04L-009/00; H04L-009/32
File Segment: EPI

29/5/24 (Item 21 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012840121 **Image available**
WPI Acc No: 2000-011953/ **200001**
Related WPI Acc No: 2001-578355
XRPX Acc No: N00-009207

Encrypted **configuration data communicating method for use in programmable logic device**

Patent Assignee: XILINX INC (XILI-N)
Inventor: ERICKSON C R
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5970142	A	19991019	US 96703117	A	19960826	200001	B

Priority Applications (No Type Date): US 96703117 A 19960826
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5970142	A		9	H04L-009/00	

Abstract (Basic): US 5970142 A

NOVELTY - A key is pseudo randomly generated in a programmable logic device (PLD) (110) and is transmitted to a storage device. An **encrypted** configuration data generated from original configuration data in storage device (120) is transmitted to PLD. **Encrypted** configuration data is **decrypted** to produce original configuration data which originally configures PLD.

DETAILED DESCRIPTION - **Another key** is pseudo randomly **generated** and transmitted from PLD to a storage device. Additional **encrypted** configuration data is generated using the key and is transmitted to PLD. The additional **encrypted** data is **decrypted** and additional original configured data is generated. The PLD is configured using additional original configuration data, produced after **decryption** . An INDEPENDENT CLAIM is also included for programming apparatus for programmable logic device.

USE - For communicating **encrypted** configuration data between PLD and storage device.

ADVANTAGE - Uses relatively small number of gates and provided adequate protection of the circuit design as implemented in PLD.

DESCRIPTION OF DRAWING(S) - The figure shows PLD and storage device having security circuits.

PLD (110)

Storage device (120)

pp; 9 DwgNo 1/3

Title Terms: **ENCRYPTION** ; CONFIGURATION; DATA; COMMUNICATE; METHOD; PROGRAM; LOGIC; DEVICE
Derwent Class: T01; U21; W01
International Patent Class (Main): H04L-009/00
File Segment: EPI

29/5/25 (Item 22 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012837224 **Image available**
WPI Acc No: 2000-009056/ 200001
XRPX Acc No: N00-008285

Common key generating system in transmitting and receiving apparatus for IC card - generates common key generation value and common key generation information which are transmitted to next party

Patent Assignee: MATSUSHITA DENKI SANGYO KK (MATU)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 11289324	A	19991019	JP 9891169	A	19980403	200001	B

Priority Applications (No Type Date): JP 9891169 A 19980403
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 11289324	A		10	H04L-009/08	

Abstract (Basic): JP 11289324 A

NOVELTY - A common key generation unit (107) generates a common key, based on the common key generation value stored in a common key value register (103) and the common key generation information stored in the common key generation information register (105). The common key generation value and information are then transmitted to the other party. DETAILED DESCRIPTION - **Another** common **key** is **generated** using the **next** common **key** **generation** value and the common key **generation** information stored in the **next** common **key** **generation** value register (104) and the common key **generation** information register, respectively. Then, the **next** common **key** **generation** value and information are transmitted. An INDEPENDENT CLAIM is also included for transmitting and receiving procedure.

USE - In transmission and reception of an IC card system.

ADVANTAGE - Since the common key generated which is used for **encrypting** data is not transmitted, the confidentiality of the transmitted and received data is enhanced. DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the IC connection card. (103) Common key value register; (104) Common key generation register; (105) Common key generation information register; (107) Common key generation unit.